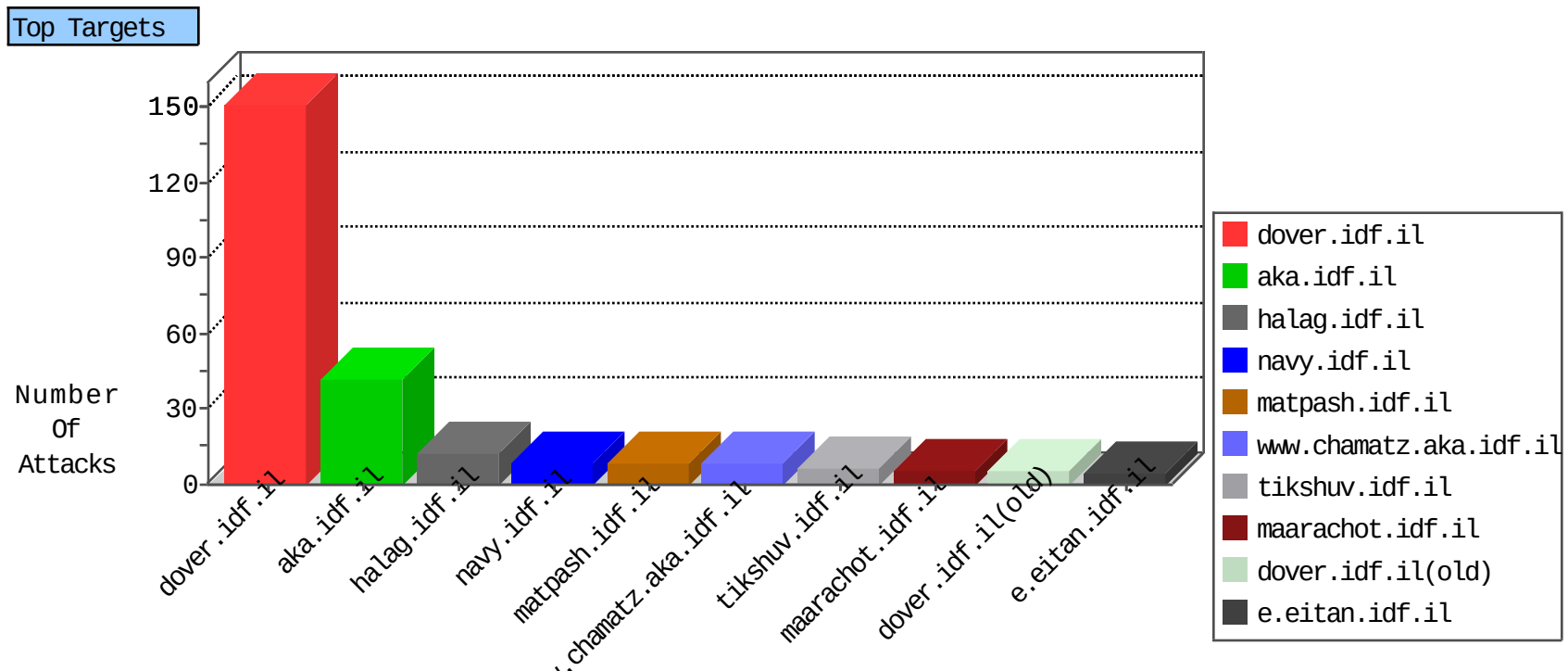
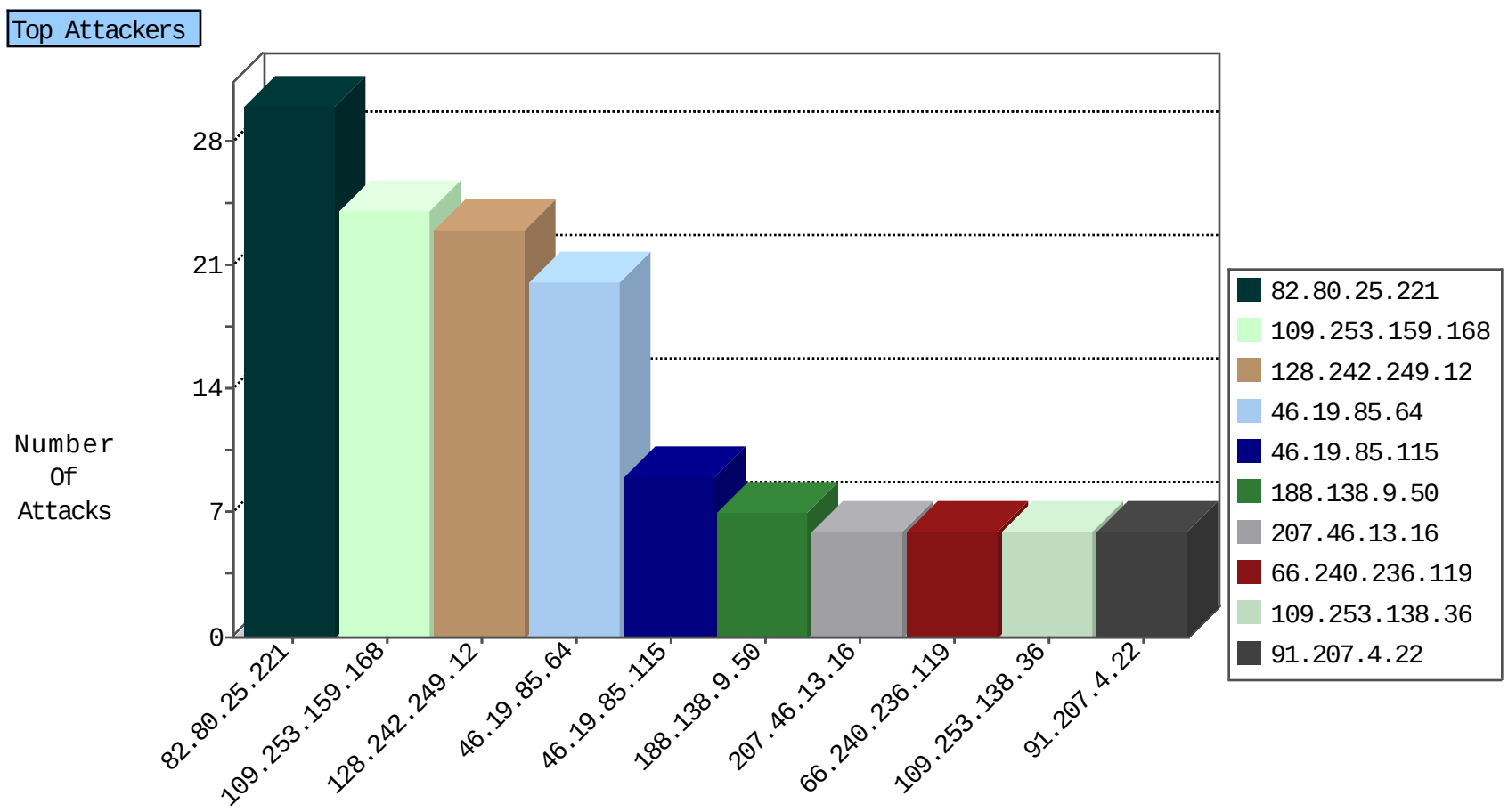
03-31-2015-01:03:03 to 03-31-2015-02:03:03

IDF Under Attack
03-31-2015-01:03:03

Top Targets



Top Attackers



03-31-2015-01:03:03 to 03-31-2015-02:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
85.25.43.94	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
192.187.107.2	United States	147.237.77.61	e.cogat.idf.il	Invalid L4 Header Length	drop	1
121.229.220.117	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
23.95.248.132	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
183.136.216.7	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

03-31-2015-01:03:03 to 03-31-2015-02:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	23
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
91.207.4.22	Ukraine	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	6
188.138.9.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	2
37.247.97.194	Turkey	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	2
93.120.27.62	Romania	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
175.44.5.185	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1

03-31-2015-01:03:03 to 03-31-2015-02:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
186.120.99.242	Dominican Republic	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
186.120.99.242	Dominican Republic	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
125.88.17.137	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
104.155.192.40		147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
222.69.94.13	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
61.158.162.40	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
37.247.97.194	Turkey	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
186.120.99.242	Dominican Republic	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
183.136.216.7	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.155.192.40		147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
103.238.214.79		147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.129.101	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
37.247.97.194	Turkey	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1

03-31-2015-01:03:03 to 03-31-2015-02:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.253.159.168	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
46.19.85.115	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.138.36	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
109.253.146.89	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.210.186.153	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.19.85.64	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
157.55.39.41	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
84.109.112.108	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.85.64	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
46.120.173.223	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
37.46.39.131	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
188.120.148.196	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
62.210.82.105	France	147.237.72.14	dover.idf.il(old)	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
79.176.190.43	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
66.249.75.96	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
82.145.222.172	Europe	147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	2
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.75.112	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
5.102.254.218	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
141.212.122.14	United States	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
93.172.16.2	Israel	147.237.72.166	aka.idf.il	illegal header format detected: Malformed HTTP protocol name in response	Block HTTP Non Compliant	monitor	1
146.185.239.104	Russian Federation	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
175.44.5.185	China	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
46.120.173.223	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
180.76.6.225	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
84.228.58.104	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

03-31-2015-01:03:03 to 03-31-2015-02:03:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.108.31.21	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.108.31.21	Block	5
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	4
91.200.12.139	Ukraine	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	2
46.19.86.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.172.16.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
54.167.176.81	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.167.176.81	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
176.219.142.119	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
72.70.53.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	1
188.165.15.121	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1244-he/atal.aspx	Block	1
84.108.31.21	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/6_s3_	Block	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/iaf/669.stm	Block	1
120.15.33.201	China	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 120.15.33.201	Block	1
77.125.150.144	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
54.167.176.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/may/19.stm	Block	1
188.165.15.148	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
84.228.196.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
120.15.33.201	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums/searchresults.aspx/trackback/	Block	1
79.176.190.43	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.176.190.43	Block	1
61.18.88.167	Hong Kong	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9825-he/refuah.aspx	Block	1
85.65.160.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/592-4071-en/sb_item_lev1	Block	1
37.142.148.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter itemid in www.aka.idf.il/kamlar/gallery/showpicture.asp	None	1
84.94.79.247	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
61.18.88.167	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1

03-31-2015-01:03:03 to 03-31-2015-02:03:03